Davis Polk

CFIUS update: Biden administration priorities

September 23, 2022 | Client Update | 9-minute read

A new Executive Order summarizes CFIUS's approach to national security issues, and CFIUS's 2021 report provides a window into recent trends.

On September 15, 2022, the Biden administration issued an Executive Order (EO 14083), directing the Committee on Foreign Investment in the United States (CFIUS or the "Committee") to consider specific risks when reviewing covered transactions.[1] While these risks are familiar to close observers of the CFIUS process, the new guidance underscores areas of emphasis and the continued expansion of national security analysis into the broader U.S. economy. CFIUS's annual report for 2021, released in August and briefly summarized here, provides additional insight into the evolution of the CFIUS process after the 2018 adoption of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) and its implementing regulations.

EO 14083 defines five new national security factors and elaborates on existing statutory factors. It does not, however, change CFIUS's existing processes or legal jurisdiction, and as noted, it largely reflects areas of emphasis familiar from recent CFIUS reviews and other Biden administration initiatives: supply chain security (inside and outside the defense industry), U.S. technological leadership, cybersecurity, and personal data. EO 14083 thus fits into the Biden administration's emphasis on supporting critical industries and supply chains in the United States.[2]

CFIUS's annual report to Congress likewise provides a useful window into CFIUS trends. Notable takeaways from 2021 include:

- a significant increase in transactions withdrawn and refiled, which extends the formal CFIUS process beyond the statutory timetable;
- continued high levels of activity in the CFIUS unit that investigates transactions that are not voluntarily notified;
- an uptick in Chinese investments subject to CFIUS review, reversing recent trends; and
- an increased use and success of CFIUS's short-form declaration procedure.

Summary of EO 14083 – National security factors

EO 14083 elaborates and expands upon national security factors for CFIUS to consider. The factors set out in EO 14083 are: (1) U.S. supply chain resiliency; (2) U.S. technological leadership; (3) aggregate investment trends; (4) cybersecurity; and (5) sensitive personal data. In addition, EO 14083 directs CFIUS to consider "relevant third-party ties," meaning ties to "foreign persons, including foreign governments, to whom the foreign person has commercial, investment, non-economic, or other ties (relevant third-party ties) that might cause the transaction to pose a threat to national security."[3]

We have elaborated on each of these factors below.

Factor 1 – Resilience of critical U.S. supply chains

The first factor concerns a transaction's effect on supply chain resilience and security. This consideration explicitly extends to supply chains outside the defense industrial base (the original focus of CFIUS), echoing the Biden administration's earlier Executive Order directing agencies across the Executive Branch to develop plans to strengthen the U.S. domestic supply chain for a number of industries, including elements of the technology sector, clean energy and climate adaptation, critical minerals, and food security.[4] According to the White House Fact Sheet, critical U.S. supply chains may become vulnerable to future disruptions if "an investment shifts ownership, rights, or control with respect to certain manufacturing capabilities, services, critical mineral resources, or technologies" that are fundamental to national security, to a foreign person who might take actions that threaten to impair U.S. national security as a result of the transaction.[5] To assess whether a covered transaction might undermine the resilience and security of critical supply chains, CFIUS will consider, among other things, the degree of diversification through alternative suppliers; whether the U.S. party to the transaction supplies the United States Government; and the concentration of ownership or control by the foreign person in a given supply chain. This factor explicitly brings into CFIUS's purview non-defense supply chain vulnerabilities of the U.S. economy highlighted by pandemic-related disruptions and addressed by other recent U.S. policy initiatives, such as the CHIPS and Science Act.[6]

Factor 2 – U.S. technological leadership

The second factor is a transaction's effect on U.S. technological leadership in areas affecting national security. EO 14083 identifies "microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, and climate adaptation technologies" as sectors that are fundamental to U.S. technological leadership. EO 14083 also directs the Committee to consider whether a covered transaction could reasonably result in future advancements and applications in technology that could undermine national security. CFIUS's consideration will be informed by periodic reports from the Office of Science and Technology Policy identifying technology sectors that it "assesses are fundamental to United States technological leadership in areas relevant to national security" and by the Commerce Department's ongoing identification of emerging and foundational technologies pursuant to the Export Control Reform Act of 2018 and FIRRMA. [7]

Factor 3 – Aggregate industry investment trends

Recognizing that a coordinated strategy to acquire related technologies or companies may have a cumulative impact, EO 14083 directs the Committee to evaluate transactions in the context of related transactions, particularly transactions in a single industry sector or that involve related manufacturing capabilities, services, critical mineral resources, or technologies. The Committee has statutory authority to consider this broader context pursuant to Section 1702(c)(2) of FIRRMA, which authorizes CFIUS to assess "the cumulative control of, or pattern of recent transactions involving, any one type of critical infrastructure, energy asset, critical material, or critical technology by a foreign government or foreign person" in assessing national security risks. Heightened attention to trends may also provide CFIUS with another basis to initiate retroactive reviews of deals that closed without a CFIUS filing.

Factor 4 – Cybersecurity risks

EO 14083 directs the Committee to consider whether a covered transaction erodes U.S. cybersecurity by providing a foreign person with the opportunity to conduct cyber intrusions or other malicious cyber-enabled activity. Such activities include those designed to affect the outcome of any election for Federal, State, Tribal, local, or territorial office; the operation of United States critical infrastructure; or the confidentiality, integrity, or availability of United States communications.

Factor 5 – U.S. persons' sensitive data

In recent years, CFIUS has increasingly been concerned with "big data" and the risk that hostile actors could collect and mine data on U.S. persons for intelligence, targeting, and other purposes. FIRRMA reflected this focus, identifying the exploitation of sensitive personal data as a potential national security risk,[8] and creating relatively narrow mandatory filing requirements for transactions involving prescribed types and quantities of data. EO 14083 goes even further, recognizing that advances in technology, combined with access to large data sets, increasingly enables the re-identification or de-anonymization of what was once unidentifiable data to be exploited by hostile actors.

Periodic review

Section 4 of EO 14083 instructs the Committee to regularly review its processes, practices, and regulations, and to periodically provide the National Security Advisor with a report documenting the results of its review. The report should

include any resulting policy recommendations that the Committee considers necessary to meet the evolving set of national security risks.

Summary of Annual Report

On August 2, 2022, CFIUS released its Annual Report to Congress regarding its review of foreign investment transactions in calendar year 2021, the first full year under the final rules implementing FIRRMA.

Below are a few key observations from the Annual Report:

- CFIUS received 272 full notices in 2021, a significant increase from the number of notices in 2020 (187), and 2019 (231).
  - CFIUS commenced an investigation for 48 percent of the notices it received (130 of 272), a proportion that has remained relatively constant in recent years.
  - CFIUS imposed mitigation measures, often in the form of a National Security Agreement, in 10 percent of the notices it received (26 of 272), which is also approximately the same proportion as in 2020.
  - Most transactions continue to clear CFIUS review. CFIUS failed to clear just over 3% of transactions filed (9 of 272), either informing the parties that no mitigation was possible or proposing mitigation measures that were unacceptable to the parties. This is comparable to recent years (4.3% and 3.4% in 2019 and 2020, respectively) and down from a high of 10.5% in 2017. No transactions were referred to the President for decision.
  - 63 transactions (23%) were withdrawn and re-filed, which effectively extends the statutory review period (which contemplates a two-stage CFIUS process with 45 days for each stage). This is a significant increase over the 8% rate of 2019 and 2020, and is the highest in recent years. As mitigation and prohibitions have not increased, this signals an increased risk of delay in the CFIUS process.
- The recent steep decline in Chinese (ex-Hong Kong) transactions reviewed was in part reversed:

Year	2017	2018	2019	2020	2021
# of PRC transactions	60	55	25	17	44
% of all CFIUS reviews	25.3%	24.0%	10.8%	9.1%	16.1%

- The use of short-form declarations continues to increase, with 164 declarations submitted in 2021 compared to 94 in 2019 and 126 in 2020.[9]
-
  - A short-form declaration can result in either a clearance, a request to file a full notice, or no decision (meaning CFIUS in principle could re-open the transaction later, though this is rare).
  - The percentage of declarations resulting in a definitive clearance continued to increase (37% in 2019, 64% in 2020, and 73% in 2021).
  - The percentage of declarations resulting in a request for a full filing remained relatively stable (18%), while the percentage of declarations resulting in a “no decision” decreased (7%).
  - Given CFIUS is increasingly moving away from using the “no decision” option, short-form notifications are more attractive in appropriate cases.
- CFIUS’s non-notified transactions unit continues to be very active, identifying 135 transactions for CFIUS consideration that the parties did not voluntarily notify to CFIUS (up from 117 in 2020).
  - CFIUS has developed a standard questionnaire that it sends to the parties to identified non-notified transactions, which can require the production of a significant amount of information.
  - Many inquiries are resolved at the questionnaire stage; CFIUS ultimately required a full filing in only 8 of the 135 cases.
- Finally, CFIUS provided a useful, illustrative summary of mitigation measures negotiated and adopted in 2021, which included:

- prohibiting or limiting the transfer or sharing of certain intellectual property, trade secrets, or technical information;
- establishing guidelines and terms for handling existing or future contracts with the U.S. Government or its contractors, U.S. Government customer information, and other sensitive information;
- ensuring that certain facilities, equipment, data, and operations are located only in the United States;
- establishing a corporate security committee, voting trust, and other mechanisms to limit foreign influence and ensure compliance, including the appointment of a U.S. Government-approved security officer and/or member of the board of directors and requirements for security policies, annual reports, and independent audits;
- notifying customers or relevant U.S. Government parties when there is a change of ownership in the U.S. business;
- assurances of continuity of supply to the U.S. Government for defined periods, notification and consultation prior to taking certain business decisions, and reserving certain rights for the U.S. Government in the event that the company decides to exit a business line; establishing meetings to discuss business plans that might affect U.S. Government supply or raise national security considerations;
- ensuring that only authorized vendors supply certain products or services; and
- prior notification to and approval by relevant U.S. Government parties in connection with any increase in ownership or rights by the foreign acquirer.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Mary Jane Dumankaya
+1 212 450 3654
maryjane.dumankaya@davispolk.com

Kendall Howell
+1 202 962 7068
kendall.howell@davispolk.com

Paul Marquardt
+1 202 962 7156
paul.marquardt@davispolk.com

John B. Reynolds III
+1 202 962 7143
john.reynolds@davispolk.com

Charles Marshall Wilson
+1 202 962 7130
charles.wilson@davispolk.com

[1] Executive Order 14083, "Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States," 87 FR 57369.

[2] For example, EO 14017, issued in February 2021, sought to strengthen U.S. supply chains and resulted in the Departments of Commerce, Defense, Energy and Health and Human Services releasing separate reports and plans to strengthen the U.S. domestic supply chain for certain critical industries. Executive Order 14017, America's Supply Chains, 86 FR 11849.

[3] EO 14083, 87 FR 57370.

[4] Executive Order 14017, America's Supply Chains, 86 FR 11849.

[5] EO 14083 lists specific manufacturing capabilities, services, critical mineral resources, and technologies for the Committee to consider in its review of covered transactions. These include "microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy (such as battery storage and hydrogen), climate adaptation technologies, critical materials (such as lithium and rare earth elements), elements of the agriculture industrial base that have implications for food security and any other sectors identified in Executive Order 14017 of February 24, 2021 (America's Supply Chains)."

[6] 15 U.S.C. § 4651 et seq.

[7] 50 U.S.C. § 4817.

[8] According to EO 14083, sensitive personal data includes U.S. persons' health, digital identity, or other biological data and any data that could be identifiable or de-anonymized.

[9] Notably, in the Proposed FIRRMA Regulations, CFIUS predicted that there would be approximately 550 short-form declarations submitted per year.